Fachwissenschaft und Fachdidaktik Informatik

der Freien Universität Berlin

Masterarbeit

Im Masterstudiengang für ein Lehramt an Gymnasien mit dem Profil Quereinstieg

Auswirkungen von Big Data auf die Demokratie am Beispiel von politischem Wahlkampf

1. Gutachter/in (Betreuer/in): Univ.-Prof. Lutz Prechelt

2. Gutachter/in: Prof. Dr. Barbara Pfetsch

vorgelegt von: Elena Magdalena Germanidis

Matrikelnummer: 5241839

E-Mail: elena22ger@gmail.com

Berlin, 19.10.2021

Selbständigkeitserklärung
zur Abschlussarbeit

Ich erkläre ausdrücklich, dass es sich bei der von mir eingereichten schriftlichen Arbeit mit dem Titel

Auswirkungen von Big Data auf die Demokratie am Beispiel von politischem Wahlkampf

um eine von mir selbst und ohne unerlaubte Beihilfe verfasste Originalarbeit handelt.

Ich bestätige überdies, dass die Arbeit als Ganze oder in Teilen nicht zur Abgeltung anderer Studienleistungen eingereicht worden ist.

Ich erkläre ausdrücklich, dass ich sämtliche in der oben genannten Arbeit enthaltenen Bezüge auf fremde Quellen (einschließlich Tabellen, Grafiken u. Ä.) als solche kenntlich gemacht habe. Insbesondere bestätige ich, dass ich nach bestem Wissen sowohl bei wörtlich übernommenen Aussagen (Zitaten) als auch bei in eigenen Worten wiedergegebenen Aussagen anderer Autorinnen oder Autoren (Paraphrasen) die Urheberschaft angegeben habe.

Ich nehme zur Kenntnis, dass Arbeiten, welche die Grundsätze der Selbständigkeitserklärung verletzen – insbesondere solche, die Zitate oder Paraphrasen ohne Herkunftsangaben enthalten –, als Plagiat betrachtet werden können.

Ich bestätige mit meiner Unterschrift die Richtigkeit dieser Angaben.

19.10.2021 Ett Gemanidis

Datum, Name

Inhaltsverzeichnis

1.Einleitung 1
2 Datenbasierter Wahlkampf 3
2.1 Forschungsstand 4
2.2 Mikrotargeting im Wahlkampf 5
2.3 Involvierte Akteure 7
2.4 Beispiele beim Mikrotargeting angewendeter Technologien 8
3. Auswirkungen des datengetriebenen Wahlkampfs 10
3.1 Chancen von Mikrotargeting 10
3.1.1 Kritik an den positiven Effekten von Mikrotargeting 13
3.2 Risiken von Mikrotargeting 13
3.2.1 Privatsphäre 14
3.2.2 Technologiekonzerne 15
3.2.3 Öffentlichkeit 19
4. Regulierung von politischem Mikrotargeting 20
4.1 DSGVO im Kontext des politischen Wahlkampfs 22
4.1.1 Persönliche Daten sammeln 22
4.1.1 Profiling und Targeting 24
4.2 Verhaltenskodex zur Bekämpfung von Desinformation 25
4.2.1 Beispiele zur Selbstregulierung der Plattformen 26
4.2.2 Bewertung des bisherigen Kodexes 28
4.3 Europäischer Aktionsplan für Demokratie 29
4.4 EU-Digital-Service-Act 29
4.5 Zusammenfassung EU-Regulierung 30
5. Zusammenfassung und Ausblick 30
Literaturverzeichnis 32

1.Einleitung

Durch die Digitalisierung der Gesellschaft werden täglich enorme Mengen an Daten produziert, bis 2025 soll die weltweit generierte Datenmenge auf insgesamt 175 Zettabyte (175 mal 10^{21}) angewachsen sein (Seagate,2018). Solche großen Mengen an Daten, die mit herkömmlichen Datenverarbeitungssystemen nicht bewältigt werden können, werden mit dem Begriff *Big Data* bezeichnet. *Big Data* hat sich zu einem Buzzword entwickelt, dessen Definition oft vom Kontext abhängig ist. Eine der ersten Definitionen stammt von Doug Laney (2001). Er definiert *Big Data* als Daten, die die Eigenschaften *volume, velocity* und *variety* besitzen (Laney, 2001). Diese werden auch ‚drei Vs' genannt. Die Daten werden nicht nur durch ihre Größe charakterisiert, sondern auch durch ihre hohe Generationsgeschwindigkeit und Artenvielfalt. Einige Quellen benutzen inzwischen ein Modell mit fünf Vs; zusätzlich zu den drei bereits genannten kommen *veracity* und *value. Veracity,* oder auch ‚Richtigkeit', gibt Auskunft über die Qualität der Daten und ihrer Quellen. Das fünfte V entspricht dem Mehrwert der Daten (Riahi und Riahi, 2018). Die Notwendigkeit, große Menge an Daten zu verarbeiten, die in der Qualität variieren und sich schnell verändern, treibt die Entwicklung von neuen methodischen Ansätzen und Technologien an. Deswegen wird *Big Data* oft mit Technologien wie *Data Mining* und *Maschinelles Lernen* assoziiert. Neben der Notwendigkeit, große Mengen an Daten zu verarbeiten, wird der Begriff *Big Data* mit der Ambition, neue Erkenntnisse zu gewinnen und genauere Vorhersagen zu treffen verknüpft. Somit hat *Big Data* in vielen Lebensbereichen Anwendung gefunden, vom Gesundheitswesen, wie bei der Mustersuche in DNA-Sequenzen, bis zu politischen Wahlkämpfen, zum Beispiel durch den Einsatz von Mikrotargeting.

Die USA Wahlen von 2012 wurden als die „*ersten Big-Data-Wahlen*"[1] charakterisiert (Hellweg 2012). Jedoch brach nach dem Skandal von Cambridge Analytica im Jahr 2016 erneut eine große öffentliche Debatte über die Auswirkungen der Anwendung von Big Data im Wahlkampf auf die Demokratie aus, insbesondere durch Mikrotargeting. Im Jahr 2018 wurde öffentlich, wie Millionen Daten von Facebook-Nutzenden von Cambridge Analytica benutzt wurden, um Persönlichkeitsprofile zu erstellen und durch maßgeschneiderte Nachrichten die Meinung Tausender Wählender zu beeinflussen (Cadwalladr und Graham-Harrison, 2018). Dies fand

[1] Eigene Übersetzung aus dem Englischen

während der US-Präsidentschaftswahlen 2016 und der der Brexit-Abstimmung statt. Dabei wurden Wählende unter anderem durch Mikrotargeting und Psychometrisches Profiling angeblich gezielt manipuliert und somit die Ergebnisse der Wahlen beeinflusst. Die Manipulation von Wahlen ist eine Gefahr für das etablierte System repräsentativer Demokratie (Thiel, 2018). Das Forschungsprojekt Assessing Big Data (Abida) hat die medienöffentliche Debatte über die datenbasierten Wahlkämpfe in den USA, Großbritannien und Deutschland komparativ untersucht, indem es zwei Zeitungen des jeweiligen Landes inhaltlich analysiert hat. Es hat sich ergeben, dass die Meinungen über den Einsatz von Big-Data-Praktiken in Wahlkampagnen immer noch geteilt sind. Dabei haben sich die Optimisten, die Pessimisten, die Skeptiker und Warnenden als Gruppen hervorgetan (Pentzold und Fölsche, 2018). Die erste Gruppe beinhaltet Personen, die die Vorteile bei dem Einsatz solcher Techniken sehen, wie zum Beispiel eine effektive und effiziente Wahlkampagne (Pentzold und Fölsche, 2018). Dagegen zweifeln die Pessimisten an der Effektivität dieser Praktiken (Pentzold und Fölsche, 2018). Skeptiker sehen den Einsatz als vorteilhaft, aber nur als eines der Werkzeuge eines Wahlkampfs. Die Warnenden machen sich Sorgen über die möglichen negativen Auswirkungen (Pentzold und Fölsche, 2018).

Obwohl die Meinungen geteilt sind, findet diese Art von Wahlkampf in immer mehr Ländern statt. Die Forschung zum Einsatz von Big Data in Wahlkampagnen ist sehr divers gestaltet. Auch die Bedeutung des Begriffs ‚datengetriebener Wahlkampf' ist unklar, da sie im Auge des Betrachters liegt (Jessica Baldwin-Philippi, 2019). Die Gründe dafür sind vielfältig. Ein Beispiel sind die Unterschiede, die es bei der Durchführung der Wahlen und somit auch der Wahlkampagnen von Land zu Land gibt (Dobber et al., 2017). Außerdem spielen die unterschiedlichen Datenschutzgesetze eine große Rolle (Dobber et al.,2019a).

Hier wird noch einmal deutlich, wie notwendig eine intensive Auseinandersetzung mit dem Einsatz von Big-Data-Technologien im Vorfeld von Wahlen ist, um zu verstehen, wie diese eingesetzt werden, welche Auswirkungen sie haben und wie sie reguliert werden können. In Zeiten von Corona, wo der Wahlkampf durch die gegebenen Umstände größtenteils online stattfinden muss, sind die Sorgen über die Auswirkungen auf die Demokratie nicht wegzudenken.

Boyd und Crawford (2012) charakterisieren Big Data als ein komplexes „sozio-technisches Phänomen" mit weitreichenden Auswirkungen. Der technische Aspekt ist

ein fester Teil davon und erfordert entsprechende Kompetenzen von Forschenden und Anwendenden. Das bedeutet, dass immer mehr Expertinnen und Experten aus der Technologiebranche in Wahlkampfkampagnen beteiligt sind. Sie sollten auch zu einer entsprechenden Entwicklung und Regulierung dieser Anwendungen beitragen.

In dieser Masterarbeit werden, mittels einer Literaturrecherche, die Auswirkungen von Big Data auf die Demokratie eruiert. Dies erfolgt zunächst anhand der Betrachtung der Auswirkungen von Mikrotargeting im politischen Wahlkampf. Durch das Definieren von Mikrotargeting und die dazu gehörigen Komponenten, wie Akteure und gängige digitale Technologien wird die Entwicklung des datenbasierten Wahlkampfs erläutert. Danach werden unterschiedliche Meinungen über die möglichen Auswirkungen in der Fachliteratur dargestellt. Des Weiteren hat der Skandal von Cambridge Analytica und Facebook zu Veränderungen geführt, zum Beispiel in der Art und Weise wie große Technologiekonzerne an politischen Wahlkämpfen teilnehmen. Unter Betrachtung der Datenschutzgrundverordnung (DGSVO) und weiteren Maßnahmen gegen die Nutzung von Big-Data-Anwendungen ist zu beachten

2 Datenbasierter Wahlkampf

Die Anwendung von Big-Data-Technologien, um Personen zielgerichtet mit personalisierter Werbung anzusprechen, stammt ursprünglich aus dem kommerziellen Sektor. Wie Bashyakarla et al. in ihrem Bericht notieren, „verwenden politische Parteien dieselben Techniken, um den Wählenden politische Kandidaten zu verkaufen, wie die Unternehmen verwenden, um den Verbrauchern Schuhe zu verkaufen“ (Bashyakarla et al., 2019, S. 6). Dieser Übergang vom kommerziellen Werbesektor zum datenbasierenden politischen Wahlkampf wurde erstmals in den USA beobachtet. Der genaue Zeitpunkt ist schwer zu definieren, aber der erfolgreiche technologieintensive Wahlkampf von Barack Obama im Jahr 2008 und 2012 dienen als Prototypen für den datengetriebenen Wahlkampf (Kreiss 2016). Seitdem wird der datengetriebene politische Wahlkampf und demzufolge auch Mikrotargeting als ein Erfolgsfaktor gesehen.

Darüber hinaus ist wichtig anzumerken, dass bei den beiden Wahlkampagnen der Demokraten zusätzlich Personen mit technischem Hintergrund gearbeitet haben. Unter anderem zeigte Daniel Kreiss, dass diese zur Entwicklung und Anwendung technischer Innovationen und somit zum Erfolg geführt haben (Kreiss, 2016; Republican National Committee, 2013). Ein Technologievorsprung kann also

entscheidend für den Sieg sein. Eine dieser technischen Innovationen war die Entwicklung von *Narwhal* für Obamas Wahlkampf im Jahr 2012. Das Programm vereinte Daten aus zuvor getrennten Informationsquellen in einer Datenbank. Am Ende der Wahlen von 2012 beinhaltete die Datenbank von anfänglich zehn Terabyte das Fünffache an Daten (Nickerson und Rogers, 2014). Die unerwarteten Ergebnisse der USA-Wahlen 2016 sowie des Brexits haben eine große Diskussion darüber ausgelöst, inwieweit die Anwendung von Big-Data-Technologien und im Besonderen von Mikrotargeting im Wahlkampf, die Wählenden beeinflussen kann (Cadwalladr, 2017).

Der datengetriebene Wahlkampf ist inzwischen ein fester Bestandteil moderner politischer Kampagnen. Er wird weltweit angewendet: von Kanada (Lavigne, 2020) bis hier in Europa. Jedoch ist das Verständnis über den datengetriebenen Wahlkampf und insbesondere von politischem Mikrotargeting nicht ausreichend (Bennett und Gordon, 2020).

Auch die immer weiter verbreitete Nutzung von sozialen Medien ist von Bedeutung, da sie eine der primären Datenquellen sind. Nicht nur Merkmale der Nutzer können gesammelt werden, sondern auch Daten über ihr Verhalten.

2.1 Forschungsstand

Die Forschung über politisches Mikrotargeting bezieht sich hauptsächlich auf die USA da dort seine Anwendung gängiger ist. Die Gründe weshalb Mikrotargeting so verbreitet in den USA ist, sind divers. Als erstes erlauben die rechtlichen Bedingungen den amerikanischen Parteien das Sammeln und Speichern von großen Mengen an persönlichen Daten (Papakyriakopoulos et al.,2018). Zweitens unterscheiden sich die Budgets für Wahlkampagnen von denen hier in Europa enorm (Baldwin-Philippi, 2019). Außerdem sind die USA der Stammsitz vieler großer technologischer Konzerne wie zum Beispiel Facebook, welche Mikrotargeting auf ihren Plattformen anbieten und antreiben (Kreiss und Mcgregor, 2018).

Die Forschung über Mikrotargeting in Europa ist überschaubar. Nur wenige Forschungen untersuchen den Einsatz von Mikrotargeting im Wahlkampf in Europa. Studien haben gezeigt, dass auch Europäische Parteien vom berüchtigten Erfolg des Mikrotargeting in den USA profitieren wollen und ähnliche Strategien umsetzten (Bennett 2018; Kruschinski und Haller 2017). Studien die politische Werbung auf

Facebook während der Europa Wahlen untersucht haben, haben herausgefunden, dass Mikrotargeting nur begrenzt eingesetzt wird (Ortega, 2020; Serrano et al.,2020). Weitere Forschung wird benötigt, um den Einsatz von Mikrotargeting und seine Auswirkungen im europäischen Kontext zu verstehen.

Der Hintergrund für eine unzureichende Forschung auf dem Gebiet des Mikrotargeting kann die Tatsache sein, dass diese Methode der gezielten Ansprache noch nicht lange in Europa praktiziert wird. Auch ein Mangel an erforderlichen Daten, schränkt die Forschenden bei ihren Recherchen ein. Seit 2019 sind in Europa Werbearchive von großen Plattformen erstellt worden, diese können die Forschung vorantreiben. Einige der oben genannte Studien haben diese Werbearchive auch genutzt.

Hier wäre eine interdisziplinäre Zusammenarbeit sinnvoll, um die Entwicklung neuer Anwendungen bei der Datensammlung, deren Bereitstellung und Zugänglichkeit zu ermöglichen.

Als nächstes wird der Begriff Mikrotargeting definiert, um seine Auswirkungen besser zu verstehen.

2.2 Mikrotargeting im Wahlkampf

Die Nutzung von Daten zur gezielten Ansprache von Wählern ist keine neue Strategie des Wahlkampfs. Anhand der technologischen Entwicklungen jedoch hat sich die Art seiner Durchführung weiterentwickelt. Die Konzeptualisierung der Nutzung von Big Data im Wahlkampf hat sich unterschiedlich ausgeprägt. Tufekci zum Beispiel definiert "*Computational Politics"* als

"applying computational methods to large datasets derived from online and off-line data sources for conducting outreach, persuasion and mobilization in the service of electing, furthering or opposing a candidate, a policy or legislation "(Tufekci 2014, S. 4).

Baldwin-Philippi beschreibt „*Data-driven Campaigning"* als "die Nutzung von Big Data, um entweder gezielte Nachrichten an bestimmte Bevölkerungsgruppen zu schicken oder um Tests durchzuführen, die die Effizienz unterschiedlicher Nachrichten und Ziele messen"[2] (Baldwin-Philippi 2019, S. 2). Obwohl datengetriebener Wahlkampf nicht mit Mikrotargeting gleichgesetzt werden kann, überlappen sich die Definitionen oft. Dobber et al. definieren "*Political Behavioral Microtargeting"* als die Nutzung von

[2] Eigene Übersetzung aus dem Englischen

Technologien, um Informationen über die Wählende zu sammeln und zu analysieren, um somit gezielt Personen mit personalisierten Nachrichten anzusprechen (Dobber et al., 2017, S. 2). Das Wort *behavioral* in dieser Definition beschreibt, dass die Daten aus dem vorherigen Online-Verhalten der Person stammen (Dobber et al., 2017, S. 3). Ähnlich charakterisiert es das Information Commissioners Office (ICO). Mikrotargeting

„It describes targeting techniques that use data analytics to identify the specific interests of individuals, create more relevant or personalised messaging targeting those individuals, predict the impact of that messaging, and then deliver that messaging directly to them "(ICO, 2018, S. 27).

Das ICO beschreibt zusätzlich, dass die Wirksamkeit der Nachrichten vorherbestimmt werden kann. Zuiderveen Borgesius et al. definieren "*Online Political Microtargeting"* als eine Art personalisierter Kommunikationsmethode, die das Sammeln persönlicher Informationen und das Nutzen dieser Informationen beinhaltet, um Personen gezielte politische Werbung zu zeigen (Zuiderveen Borgesius et al., 2018, S. 82). Aus dieser Definition wird ersichtlich, dass obwohl Daten online und offline gesammelt werden, wie Tufekci beschreibt das Senden der Botschaft online stattfindet. Es handelt sich also meist um politische Online-Werbung.

Für die Zwecke dieser Masterarbeit wird politisches Mikrotargeting (für bessere Lesbarkeit ab jetzt nur Mikrotargeting) anhand von vier Schritten definiert (für 1- 3 , Dobber et al. 2019a, S.2). Diese sind:

1. Sammeln von persönlichen Daten aus vielen und unterschiedlichen Quellen
2. Analysieren der Daten, um anhand ihrer Merkmale Gruppen von Personen zu identifizieren, die wahrscheinlicher auf eine bestimmte Nachricht reagieren
3. Senden der personalisierten Nachricht, meist online
4. Durch Testen Optimierung der Targeting-Strategie

Durch Mikrotargeting wird versprochen, die richtige Person im richtigen Moment über das richtige Medium mit der richtigen Botschaft erreichen zu können. Das *mikro* in Mikrotargeting ist nicht zwingend so zu verstehen, dass die Zielgruppe sehr klein ist. Obwohl häufig behauptet wird, dass Mikrotargeting auf einem präzisen segmentierten Publikum, einem bestimmten Ort und vor allem einer maßgeschneiderten politischen Botschaft beruht (Bennett und Gordon, 2020). Es bezieht sich vielmehr auf die

Homogenität einer sehr genau definierten Zielgruppe. Somit erhält eine spezifische Zielgruppe eine Botschaft, die auf eine oder mehrere ihrer Eigenschaften zugeschnitten ist (Dobber et al., 2019a). Dies kann bei Einzelpersonen den Eindruck erwecken, als würden sie persönlich angesprochen. Da die Daten außerdem auf dem Individuum beruhen und nicht auf dem *Medianwähler*, kann im Vergleich zu traditionellen Wahlkampfstrategien das gesamte Wählerspektrum angesprochen werden (Papakyriakopoulos et al., 2017).

Das Ziel jeder politischen Wahlkampfkampagne ist es, die meisten Stimmen zu gewinnen. Mikrotargeting kann dazu beitragen, indem potenzielle Wählerinnen und Wähler von einer Partei oder Politiker überzeugt werden. Außerdem kann durch Mikrotargeting informiert und mobilisiert werden. Es kann auch eingesetzt werden, um den gegenteiligen Effekt zu erzeugen, nämlich um bestimmte Wählerinnen und Wähler abzuschrecken oder zu verunsichern und zuletzt zu demobilisieren (Dobber et al., 2019a). Wie sich der Einsatz von Mikrotargeting im Wahlkampf auf die Demokratie auswirkt kann, wird im folgenden Kapitel näher behandelt.

2.3 Involvierte Akteure

Im Bericht über online geschaltete politische Werbung und Mikrotargeting von International IDEA [3] wurden folgende involvierte Akteure identifiziert: politische Parteien, politische Aktivisten, Plattformen, Databroker und politische Berater (International IDEA, 2020). Diese Aufzählung hat den Zweck, einen Überblick über die involvierten Akteure zu schaffen, die reguliert werden sollen. Die Bürgerinnen und Bürger werden zwar nicht als Akteure genannt, aber bilden den Mittelpunkt. Denn sie sind diejenigen, die die benötigten Daten produzieren, anhand derer Mikrotargeting betrieben wird. Außerdem sind sie es, die von den unterschiedlichen politischen Akteuren angesprochen werden.

Die politischen Aktivisten werden in dieser Arbeit nicht behandelt, da hauptsächlich die Anwendung von Mikrotargeting von politischen Parteien und den von ihnen verwendeten Werbediensten in ihren Wahlkampfkampagnen betrachten werden.

Databroker sammeln ständig Daten über Bürgerinnen und Bürger. Diese kombinieren sie mit weiteren – oft gekauften – Daten und erzeugen daraus Profile über sie. Diese Profile werden laufend aktualisiert und an die politischen Parteien verkauft. Zu dieser

[3] Abkürzung für: The International Institute for Democracy and Electoral Assistance (International IDEA

Kategorie lassen sich auch Technologiefirmen zählen, die sich auf die Unterstützung von politischen Kampagnen spezialisiert haben. Zu dieser Kategorie werden auch weitere Akteure wie Analysten-Firmen gezählt. Technologische Firmen spielen eine zunehmende Rolle im politischen Wahlkampf. Zusätzlich zu den großen sozialen Plattformen, die u. a. für ihre Werbeleistungen genutzt werden, gibt es mindestens 500 weitere technologische Firmen, die sich mit politischen Kampagnen befassen (Macintyre, 2021). Diese werden dadurch charakterisiert, dass sie persönliche Daten für politisches Mikrotargeting nutzen und technische Werkzeuge für die Parteien bieten, die diese selbst nicht beherrschen oder besitzen. Charakteristische Beispiele solcher Firmen sind Cambridge Analytica oder Nationbuilder. Das Europäische Parlament hat Nationbuilder bei den Europawahlen 2019 damit beauftragt, mehr Menschen zur Stimmenabgabe zu bewegen (Fanta, 2019).

Plattformen wie Facebook und Google haben in diesem Kontext unterschiedliche Rollen zu erfüllen. Sie bieten ihre Dienste zur politischen Werbung, sammeln und beobachten die Wählerinnen und Wähler und sind auch ein digitaler Ort, an dem politische Kommunikation stattfindet. Diese komplexe Rolle von sozialen Plattformen im politischen Wahlkampf wird oft als problematisch für die Demokratie gesehen (siehe Kapitel 3.2.2).

Die Parteien vollziehen nicht jeden Schritt des Mikrotargeting selbst, sondern holen sich meist Hilfe von Experten. Daten selbst zu sammeln und auszuwerten erfordert große Ressourcen, die nicht für jede Partei selbstverständlich sind. In dem Fall können die Parteien direkt von Datenbrokern oder großen Plattformen Daten und Werbedienste kaufen. Zusätzlich können sie eine Reihe von Firmen nutzen, die sich auf technologieintensiven Wahlkampf spezialisiert haben.

2.4 Beispiele beim Mikrotargeting angewendeter Technologien

Da unterschiedliche digitale Technologien beim Mikrotargeting angewendet werden, werden nachfolgend einige der gängigen Anwendungen vorgestellt. Die digitalen Technologien und Werkzeuge, die im Wahlkampf angewendet werden, werden auch als „Politechs“ bezeichnet (Chester und Montgomery, 2019, S. 3). Wie die Daten und die dazugehörigen digitalen Technologien im Wahlkampf genutzt werden, ist ein noch unvollständig erforschter Bereich, vor allem in Europa. Die ständige Weiterentwicklung neuer digitaler Technologien, die eingesetzt werden können, erschwert es, einen

Überblick zu gewinnen. Eine erste Beobachtung zeigt, dass zahlreiche dieser Verfahren aus dem Marketingbereich stammen.

‚Digital Listening' beschreibt den Prozess, veröffentlichte Daten aus sozialen Medien zu sammeln und zu analysieren (Bashyakarla et al., 2019, S. 64). Dabei werden Informationen über das Verhalten der Nutzenden gesammelt. Nicht nur die ‚Likes', sondern auch der Inhalt der Kommentare oder Posts wird analysiert. Dadurch lassen sich zum Beispiel mit Kampagnen Einsichten über die Meinungen der Wählerschaft zu einem politischen Thema zu einem bestimmten Zeitpunkt gewinnen (Bashyakarla et al., 2019).

‚Lookalike-Modelling' erlaubt es Werbetreibenden, Gruppen von Personen zu identifizieren, die ähnliche Attribute wie ihre ‚wertvollsten Kunden' aufweisen (Chester und Montgomery, 2017). Facebook bietet diese Möglichkeit durch seine ‚Lookalike-Audience'-Dienste. Dabei werden Zielgruppen mit ähnlichen demografischen Eigenschaften, Verhalten und Interessen identifiziert (Facebook,2021a). Google bietet vergleichbare Dienste zum Targeting von ‚Similar Audiences' an. Diese Instrumente werden im politischen Wahlkampf genutzt, um die potenzielle Wählerschaft zu erkennen und zu kontaktieren.

Eine weitere Targeting-Option ist Dienste, die anhand von persönlich identifizierenden Informationen wie E-Mail-Adressen spezifische Wählergruppen bilden. Facebooks ‚Custom- Audience'-Funktion erlaubt es Werbetreibenden, zusätzlich eigene Datenquellen hochzuladen, um mit diesen sowie den Facebook-Daten Zielgruppen zu bilden. Twitter und Google bieten entsprechende Dienste an.

‚Digitale Identitäten', die durch Identifizierungspraktiken erzeugt werden, ermöglichen die Erstellung eines detaillierten Profils (vgl. Strauß, 2020, S. 85). Dies erlaubt es, eine Person unabhängig über unterschiedliche Onlinedienste und Geräte wiederzuerkennen. Somit können Werbetreibende Wahlberechtigte über unterschiedliche Medien gezielt ansprechen. Dies wird als ‚Cross-Device-Targeting' bezeichnet (Chester und Montgomery, 2017).

‚Geotargeting' nutzt die Standortinformationen, um Personen mit personalisierten Werbeanzeigen anzusprechen. Durch die Standortinformationen einer Person können Rückschlusse auf ihr Verhalten und ihre Interessen gezogen werden, zum Beispiel, wo sie arbeitet oder ob sie oft das Kino besucht (Bashyakarla et al., 2019).

Eine weitere Targeting-Methode, die sogenannte Psychometrie, geht auf das OCEAN-Modell zurück und basiert auf den Persönlichkeitsmerkmalen einer Person (Srauß, 2020, S.94). Das OCEAN-Modell beschreibt fünf die durch fünf Eigenschaften: Offenheit, Gewissenhaft, Geselligkeit, Verträglichkeit und Neurotizismus (Srauß, 2020, S.94). Dadurch können politische Werbetreibende den Inhalt der Nachrichten an den Persönlichkeiten der Zielgruppe ausrichten und die Wahlberechtigten dadurch effektiver beeinflussen (Zarouali et al., 2020).

Eine andere Methode, die beim Mikrotargeting eingesetzt wird, sind A/B-Tests. Dabei handelt sich um Echtzeitexperimente, die meist in den sozialen Medien stattfinden. Es werden mehrere Versionen einer Werbeanzeige an Personen getestet. Die Reaktionen werden in Echtzeit gemessen und es wird die erfolgreichste Version bestimmt (Tufekci, 2014). Facebook bietet den Dienst *Dynamische Anzeigengestaltung* an, der von einer Werbeanzeige automatisiert neue personalisierte Varianten erstellen kann (Facebook 2021e). Die Erzeugung und das Testen einer Werbeanzeige kann zusammen voll automatisiert erfolgen.

Der automatisierte Prozess, Anzeigen mittels algorithmischer Prozesse in digitalen Medien zu kaufen und zu platzieren, nennt sich ‚Programmatic Advertising' (Chester und Montgomery, 2017). Dabei finden in Echtzeit Auktionen statt, die weniger als eine Sekunde dauern, um den Platz einer Werbung zu sichern.

Beim Einsatz von Mikrotargeting im Wahlkampf werden alle genannten Methoden kombiniert, um die Wählerschaft optimal anzusprechen.

In diesem Kapitel würde der konzeptuelle Rahmen gesetzt in dem politisches Mikrotargeting für dieser Arbeit relevant ist. Im folgenden Kapitel werden anhand dessen die möglichen Auswirkungen präsentiert.

3. Auswirkungen des datengetriebenen Wahlkampfs

Die Charakteristika von Mikrotargeting bieten sowohl Chancen als auch Risiken für die Demokratie im Kontext des politischen Wahlkampfs.

3.1 Chancen von Mikrotargeting

Die Anwendung von Mikrotargeting im politischen Wahlkampf bietet Chancen für die Demokratie. Im vorherigen Kapitel wurden eine Reihe von Mikrotargeting-Techniken präsentiert, mit welchen politische Kampagnen sowie Kandidaten und Kandidatinnen

einen immer detaillierteren Einblick in die Meinungen, Bedürfnisse und Neigungen der Wählenden gewinnen können. Dadurch ergibt sich personalisierte politische Werbung, die Personen mit für sie relevante Informationen vermittelt.

Zuiderveen Borgesius et al. (2018) argumentieren, dass Mikrotargeting Demokratie verstärken kann, indem die politische Partizipation der Bürgerinnen und Bürger erhöht wird. Wählende bekommen für sie maßgeschneiderte Werbung, die das Interesse an politischen Themen und politischem Diskurs wecken kann. Wenn sich jemand für die Umwelt interessiert, würde die Person von allen Parteien Informationen zu dem entsprechenden Aspekt ihres Wahlprogramms bekommen. Dementsprechend vertieft sich auch das Wissen der Wählerschaft über bestimmte politische Themen, was wiederrum zu einer fundierteren Wahlentscheidung führen kann (Zuiderveen Borgesius et al. 2018). Ferner kann Mikrotargeting mehr Personen dazu bewegen, sich durch kleinere Aktionen wie Spenden für ihre Partei zu engagieren (Baldwin-Philippi, 2019).

Zweitens können Politiker und Politikerinnen sowie Parteien die Interessen der unterschiedlichen Bürger genauer erkennen und ansprechen. Politischen Kampagnen können dadurch differenzierter und effizienter durchgeführt werden. Es wird somit ein breiteres Spektrum von Wählenden angesprochen, denn die Wahlprogramme sind nicht mehr am durchschnittlichen Wählenden orientiert (Papakyriakopoulos et al. 2017). Durch den Differenzierungsgrad können auch neue Gruppen identifiziert werden, deren Interessen noch nicht vertreten werden (Bashyakarla et al., 2019). Das kann zu einer besseren Repräsentation des "Willens des Volks" führen, wodurch die demokratische Legalität von politischen Entscheidungen theoretisch verstärkt werden kann (Ulbricht, 2020). Mikrotargeting kann auch genutzt werden, um Cluster von politischen Meinungen zu spalten und somit eine größere Vielfalt von Ansichten für Bürgerinnen und Bürger zu bieten. Somit wäre Mikrotargeting eine Maßnahme gegen Filterblasen (Papakyriakopoulos et al. 2017). Jedoch kann Mikrotargeting auch den Effekt von Filterblasen verstärken, wie im Kapitel 3.2.3 zu sehen ist.

Weiterhin ist es nach Zuiderveen Borgesius et al. (2018) durch Mikrotargeting möglich, Personen zu erreichen, die als politisch inaktiv gelten und über die traditionelleren Medien wie das Fernsehen nicht zu erreichen sind. Das kann wiederum es zu einer erhöhten Wahlbeteiligung führen (Baldwin-Philippi, 2019; Zuiderveen Borgesius et al., 2018).

Eine Studie aus den USA hat weiter belegt, dass durch Mikrotargeting ein positiveres Gefühl gegenüber Kandidierenden hervorgerufen werden kann, jedoch nicht die Neigung zur Stimmabgabe. Die Forscher folgerten, dass Mikrotargeting daher ein großes Potenzial hat, die Bewertung von Kandidierenden auf persönlicher Ebene zu beeinflussen, dagegen nicht genug, um politische Überzeugungen zu ändern (Krotzek Lennart 2019). Eine weitere Studie aus den USA fand heraus, dass Mikrotargeting die parteipolitische Identität verstärken kann (Lavigne, 2020). Mikrotargeting scheint somit ein effizientes Mittel für politische Parteien zu sein, um ihre parteipolitische Unterstützung zu sichern, wenn die Person die Partei bereits wählen wollte (Lavigne, 2020). Also bietet sich für jene Partei die Chance, mittels Mikrotargeting ihre Beziehungen zu ihrer Wählerschaft zu verstärken und sie somit zu mehr politischer Partizipation zu motivieren.

Man kann außerdem verhindern, dass sich die betroffene Person die gleiche Werbung mehrmals anschauen muss (Bashyakarla et al., 2019). Durch Mikrotargeting können auch bestimmte Gruppen absichtlich von der Ansprache ausgeschlossen werden, Personen, die als nicht politisch engagiert gesehen werden (Bashyakarla et al., 2019). Dies ist für die Durchführung der Kampagne positiv, denn es werden keine Ressourcen unnötig verschwendet und die bürgerliche Person wird nicht ständig von Werbung überflutet. Dieses feine Segmentieren der potenziellen Wählerschaft kann entweder als positive oder als negative Auswirkung betrachtet werden (siehe Kapitel 3.2.3).

Eine weitere Entwicklung ist, dass die meist geringen Kosten des Mikrotargeting es für kleinere Parteien möglich gemacht haben, die oben genannte Vorteile für sich zu nutzen (Bodó et al.,2017). Dadurch kann die Kampagnen entscheiden, wie sie ihre Ressourcen am besten nutzt, um Bürger und Bürgerinnen anzusprechen: Welche Wählende lohnt es sich anzusprechen, zu welchen Zeitpunkt, mit welcher Botschaft und durch welches Medium (Kruschinski und Haller, 2017). Ein weiterer Vorteil ist, dass es durch das A/B-Testen für politische Kampagnen möglich ist, die Wirksamkeit ihrer Nachrichten zu überprüfen. Ein solches Beispiel ist das Testen von unterschiedlichen Inhalten der personalisierten Nachrichten oder der Platzierung dieser auf der Webseite der Partei, um somit ein erhöhtes Engagement der Nutzerinnen und Nutzer zu erreichen (Tufekci, 2014). Durch diese auch oft in Echtzeit stattfindenden Experimente können die Kampagnen ihre Strategien optimieren, indem sie anhand der Reaktionen der Bürgerinnen und Bürger ihre Strategien anpassen.

Zusammengefasst bietet sich aus Sicht der Parteien die Chance, einen Wahlkampf zu führen, der effektiv ist und relativ niedrige Kosten benötigt. Zugleich erlangen die Parteien durch das Mikrotargeting einen tieferen Einblick in ihre Wählerschaft und haben somit die Möglichkeit, sie besser zu repräsentieren. Für die wahlberechtigten Bürgerinnen und Bürger ergibt sich die Chance, schneller und einfacher ein zu ihren Interessen passendes Wahlprogramm zu finden. Somit kann sich die politische Partizipation erhöhen. Zuletzt gibt es die Möglichkeit, eine Vielfalt an politischen Meinungen zu fördern und somit den öffentlichen politischen Diskurs zu nähren.

3.1.1 Kritik an den positiven Effekten von Mikrotargeting

Trotz der vielen Chancen, die Mikrotargeting für die Demokratie bietet, ist die Evidenz dafür spärlich. Dobber et al. machen auf die fehlenden Belege der positiven Auswirkungen von Mikrotargeting auf das Wahlverhalten aufmerksam (Dobber et al., 2019b). Baldwin-Philippi behauptet, dass diese Praktiken mehr Erfolg bei der Mobilisierung der Wählerschaft zur Urne und der Verbesserung der Spendenquoten haben als für Überzeugungszwecke, jemanden zur Unterstützung eines Kandidaten zu bewegen (Baldwin-Philippi, 2019). Dagegen hat eine Studie gezeigt, dass politische Werbeanzeigen die auf die Persönlichkeitsmerkmale der Bürgerinnen und Bürger abgestimmt überzeugender sind als im Gegenfall (Zarouali et. al., 2020). Jedoch inwiefern das auch im Wahlkampf stattfindet, ist unklar. Außerdem ist es, auch wenn die Mobilisierung erfolgt, nicht sicher, inwiefern dies tatsächlich im Interesse der Bürger und Bürgerinnen ist oder ob sie manipuliert werden (Burkell und Regan, 2019).

Fernerhin können einige der positiven Auswirkungen auch als negativen Auswirkungen betrachtet werden, wie es im folgenden Kapitel zu erkennen ist. Jedoch hat dies nicht dazu geführt, dass weniger Mikrotargeting angewendet wird.

3.2 Risiken von Mikrotargeting

Die Risiken, die sich durch den Einsatz von Mikrotargeting im Wahlkampf ergeben, stehen stärker im Vordergrund als die Chancen. Zahlreiche Forschende haben wiederholt die damit verbundenen Risiken für die Demokratie betont. Diese werden in diesem Kapitel dargestellt. Um den Umfang der Risiken besser zu verstehen, werden diese anhand der Eigenschaften von Mikrotargeting und der involvierten Akteure betrachtet. Als Erstes werden die Risiken aufgeführt, die aus der Bedrohung der Privatsphäre entstehen, als Nächstes diejenigen, die auf die wachsende Bedeutung

der sozialen Plattformen im politischen Wahlkampf zurückzuführen sind und zuletzt die Risiken für die Öffentlichkeit.

3.2.1 Privatsphäre

Eine Voraussetzung für Mikrotargeting ist das Sammeln und Analysieren großer Mengen personenbezogener Daten. Dies erfordert eine ständige Überwachung der Bevölkerung.

Bedenken gegenüber der Anwendung von Mikrotargeting hinsichtlich der Auswirkungen auf die Privatsphäre der betroffenen Personen haben sich bislang hauptsächlich im kommerziellen Kontext bewegt. Nun haben sie sich zu einem politischen Problem entwickelt (Bennett und Oduro Marfo, 2019).

Die Effektivität von Mikrotargeting beeinflusst nicht die Risiken, die sich daraus für die Privatsphäre ergeben, denn die Durchführung selbst erfordert eine große Menge personenbezogener Daten. Auch wenn Mikrotargeting nicht effektiv ist, ergeben sich durch seine Anwendung bereits Risiken für die Privatsphäre (Bennett und Oduro Marfo, 2019).

Privatsphäre ist von elementarer Bedeutung für die Demokratie. Sie sorgt für die politische Debatte, denn sie gibt den Menschen die Möglichkeit, eigene Meinungen zu äußern, politische Identitäten aufzubauen, frei von Überwachung und öffentlichem Druck (Kreiss, 2012).

Wenn Daten für Mikrotargeting-Zwecke veröffentlicht werden, wird die Privatsphäre der betroffenen Menschen verletzt. Neben dem aus den Medien bekannten Fall von Cambridge Analytica gibt es weitere Beispiele. In der Türkei hat im Jahr 2016 ein Hacker 50 Millionen Bürgerdaten hochgeladen. Obwohl sie aus dem Jahr 2008 stammten, ändern sich Namen oder Ausweisinformationen selten (Bashyakarla et al., 2019). Außerdem können auch aus den gesammelten Daten abgeleitete Informationen wie sexuelle Orientierung oder politische Neigungen an die Öffentlichkeit geraten (Dobber et al., 2019a). Obwohl die Daten für die weitere Verarbeitung anonymisiert werden, ist es durch technische Fortschritte möglich, sie auf die ursprüngliche Person zurückzuführen (Tufekci, 2014). Ein weiteres Problem ist, dass durch die kontinuierliche Sammlung und Verarbeitung von Daten vor allem aus den sozialen Medien sogenannte Schattenprofile erstellt werden können. Dabei handelt es sich um Profile von Personen, die kein Konto bei einem sozialen Medium besitzen. Dennoch

ist es möglich, aus anderen Datenquellen Rückschlüsse auf die persönlichen Merkmale der betreffenden Person zu ziehen. Somit kann die Entscheidung eines Individuums, sich vom Onlineraum fernzuhalten, trotzdem Risiken für seine Privatsphäre bergen (Lewandowsky et al., 2020).

Weiterhin kann die an Autonomie der Menschen verletzt werden (Anstead et al., 2018). Mikrotargeting kann stattfinden, ohne dass es der betroffenen Person bewusst ist, sodass diese auch keine Wahl hat, Mikrotargeting abzulehnen.

Wenn die Bevölkerung zunehmend ein Bewusstsein über eine mögliche Verletzung ihrer Privatsphäre durch Mikrotargeting-Methoden entwickelt, kann dies dazu führen, dass sie auch negative Einsichten über diese gewinnt. Zusammen können Datenschutzbedenken und die Einstellung gegenüber Mikrotargeting eine ‚verstärkende Spirale' bilden, die sich im Laufe der Zeit gegenseitig negativ beeinflusst (Dobber et al., 2019b). Demzufolge kann es dazu kommen, dass Wahlberechtigte ihr Verhalten ändern oder verbergen, weil sie sich überwacht fühlen, was als ‚Chilling-Effekt' bezeichnet wird (Dobber et al., 2019b; Zuiderveen Borgesius et al.,2018). Dieser kann eine informierte Wahlentscheidung behindern und sich nachhaltig auf dem Wahlprozess auswirken (Dobber et al., 2019b).

Dobber hat diese ‚verstärkte Spirale' untersucht und festgestellt, dass Personen ein aus demokratischer Sicht ungewolltes Verhalten zeigen können (Dobber et al., 2019b).

Somit kann die Verletzung der Privatsphäre durch Mikrotargeting zu negativen Auswirkungen auf die Demokratie führen. Es folgen die Risiken, die sich aus der Entwicklung von Technologie Firmen für die Demokratie ergeben.

3.2.2 Technologiekonzerne

Im Kontext des Wahlkampfs sind Technologiekonzerne wie Facebook und Google relevant, aber auch kleinere, vergleichsweise spezialisierte und datengesteuerte Technologiefirmen. Zur letztgenannten Kategorie gehören Unternehmen wie NationBuilder. Es sind jedoch nicht alle Risiken für die Demokratie auch auf diese Firmen übertragbar.

Facebook verzeichnet trotz einer Reihe von Datenschutzskandalen während seiner Einwicklung steigende Nutzungszahlen. Der Konzern, dem auch Instagram und Whatsapp gehören, hat inzwischen 2,9 Milliarden aktiven Nutzende weltweit (Facebook, 29. Juli, 2021). Große Plattformen wie Facebook und Google gewinnen

zunehmend an Bedeutung im Wahlkampf. Durch die Konzeptualisierung ihrer Geschäftsmodelle sammeln sie Daten über ihre Nutzenden. Darin enthalten sind Informationen wie Alter, Geschlecht und E-Mail-Adresse, die Menschen freiwillig preisgeben, meist bei der Erstellung eines Nutzerkontos. Jedoch werden auch Daten über Verhalten und Interaktionen der Nutzenden gesammelt. Darunter befinden sich beispielsweise die ‚Likes' auf einem Post, Kommentare, Fotos und auch die vernetzten ‚Freunde'. Zusätzlich werden über Tracking-Technologien weitere Daten wie der Standort gesammelt. Aus diesen Daten werden dann Profile erstellt, anhand derer die Werbetreibenden Mikrotargeting durchführen können.

Außerdem sind die Werbedienste dieser Plattformen unkompliziert anzuwenden. Deshalb greifen zahlreiche europäische Parteien im Wahlkampf auf sie zurück (Dobber et al., 2019b). Auch in Deutschland nutzen politische Parteien Facebook als einen ihrer zentralen Online-Kommunikationskanäle (Serrano et al., 2018). Auch kleinere spezialisierte Firmen können von politischen Parteien mit der Durchführung von Mikrotargeting beauftragt werden (Dobber et al., 2019b). Kreiss benennt drei Gründe, warum Facebook und Google trotzdem bei den bedeutendsten Kanälen für politische Werbung bleiben werden: ihre Größe, ihre Richtlinien zur politischen Werbung und ihre technologischen Fähigkeiten (Barrett et al.,2020).

Die Risiken, die sich durch die Nutzung der Mikrotargeting-Angebote dieser Technologiefirmen im Wahlkampf ergeben, lassen sich zusammenfassen in: Manipulation, Datenasymmetrie und Intransparenz sowie Unterdrückung und Diskriminierung der Wählerschaft.

3.2.2.1 Manipulation

Menschen, die in der Politik tätig sind, können Mikrotargeting nutzen, um Wahlberechtigte zu manipulieren (Zuiderveen Borgesius et al., 2018). Dafür bieten sich vor allem Plattformen wie zum Beispiel Facebook an, da die Online-Manipulation auf die Schwachstellen der Entscheidungsfindung abzielt und letztere, ohne dem Wissen der Nutzer beeinflusst wird. (Susser et al., 2019).

Matz et al. (2017) konnten mit Daten aus Facebook und Twitter psychologische Merkmale wie die ‚Offenheit' einer Person erfassen. Sie haben dann durch Messung der Reaktionen gezeigt, dass Personen, die gemäß ihren psychologischen Merkmalen angesprochen werden, intensiver auf Werbung reagieren. Zusätzlich konstatiert Gorton (2016), dass mit Experimenten das Verhalten der Nutzenden verändert werden

kann, oft ohne deren Wissen. Auch Zarouali et al. (2020) haben gezeigt, dass Menschen durch politische Werbung, die ihren eigenen Persönlichkeitsmerkmalen entspricht, stärker überzeugt werden. Mikrotargeting hat somit das Potenzial das Engagement der Wahlberechtigten zu beeinflussen.

Eine weitere Manipulationsmöglichkeit für politische Akteure wäre, nicht vorhersehbare Effekte auszulösen und diese dann zu seinen Gunsten zu nutzen (Hegelich und Medina Serrano, 2019).

Durch das Kombinieren von ‚Deepfakes' und Mikrotargeting können falsche Informationen während der Wahlen verbreitet werden (Dobber, 2021). Dabei handelt es sich mehrheitlich um realistisch wirkende Medieninhalte, wie zum Beispiel Videos von Kandidierenden, die durch Techniken der künstlichen Intelligenz abgeändert beziehungsweise verfälscht worden sind.

Ein solcher Einsatz von Mikrotargeting beeinflusst die Entscheidungsfindung der Zielpersonen und kann somit zu weiteren Implikationen bei demokratischen Wahlen führen (Zarouali et al., 2020). Außerdem können Wahlberechtigte ihr Vertrauen in politische Parteien und den demokratischen Prozess verlieren, wenn sie diese Anwendung von Mikrotargeting als invasiv erleben (Bashyakarla et al., 2019).

3.2.2.2 Informationsasymmetrie und Intransparenz

Die Geschäftsmodelle der technischen Konzerne erzeugen Informationsasymmetrien (Barrett und Kreiss, 2019; Strauß, 2020). Es werden große Mengen an Daten über die Nutzer gesammelt und Informationen daraus gewonnen. Dagegen besitzen Nutzer wenig Wissen darüber, wie diese Konzerne oder politische Parteien mit ihren Daten umgehen. Dies hat unterschiedliche Auswirkungen.

Es besteht (Dadurch ergibt sich) eine Intransparenz der Prozesse dieser Konzerne. Es ist schwierig für die Öffentlichkeit und Forschenden an Informationen über Mikrotargetingprozesse zu gelangen, um deren Einsatz überwachen zu können (Barrett und Kreiss, 2019). Strauß (2020) behauptet, dass nicht nur die Plattformen von der Informationsasymmetrie profitieren, sondern jeder Mensch, der die Werbedienste nutzt, darunter auch politische Parteien, die Mikrotargeting anwenden.

Diese Asymmetrie führt auch dazu, dass politische Parteien, die sich auf Dienste von Plattformen verlassen, mit unerwarteten Änderungen der Regeln rechnen müssen. Dies kann in der Folge den politischen Wahlkampf erschweren. Während der

Europawahlen 2019 etablierte Facebook beispielsweise neue Geschäftsbedingungen, die dazu führten, dass politische Werbeanzeigen nicht in allen 28 Mitgliedsstaaten der Europäischen Union möglich waren. Es dauerte drei Wochen, bis die diese Regeln auf Druck der Parteien wieder aufgehoben wurden (Dobber et al., 2019a).

Schließlich ist die Weise inkohärent, wie technische Firmen mit politischen Akteuren umgehen. Während Facebook sich aus der aktiven Beraterrolle bei Kampagnen zurückgezogen hat, erweitert Google seine Dienstleitungen. Dies stellt die Wahlgerechtigkeit infrage (Baldwin-Philippi et al., 2020). Eine Studie hat gezeigt, dass Repräsentanten von Facebook und Google als digitale Berater im Wahlkampf der beiden großen USA Parteien im Jahr 2016 mitgewirkt haben und somit die Wahlkampfstrategien mitgestaltet haben (Kreiss und McGregor,2018). Technologie Firmen spielen eine immer größere Rolle im politischen Wahlkampf, während sie jedoch einen Informationsvorsprung bewahren.

Für die Wählerschaft hat dagegen diese Asymmetrie negative Folgen. Die Menschen besitzen weder genügend Kontrolle über ihre Daten noch ausreichendes Wissen darüber, wie gezielt sie angesprochen werden.

3.2.2.3 Unterdrückung und Diskriminierung der Wählerschaft

In den vorherigen Kapiteln (3.1) wurde die Fähigkeit von Mikrotargeting als Chance für die Demokratie vorgestellt, bestimmte Gruppen von Wahlberechtigten anhand ihrer Interessen zu beeinflussen. Die gleiche Eigenschaft kann jedoch genutzt werden, um bestimmte von den Parteien ausgewählte Gruppen gezielt zu unterdrücken. Ein Bericht von „The Guardian“ beschreibt, wie die Wahlkampagne von Trump gezielt 3,5 Millionen schwarze Amerikaner, mit negativen Nachrichten über Hillary Clinton auf Facebook, vom Wählen abgehalten hat (Sabbagh, 2020).

Auch Diskriminierung bestimmter Gruppen von Wahlberechtigten durch algorithmische Entscheidungen ist eine negative Auswirkung von Mikrotargeting. Bevor Facebook durch externe Beobachtende darauf aufmerksam gemacht wurde, war für Werbetreibende das folgende Auswahlkriterium verfügbar: ‚Personen, die sich für Hass gegen Juden interessieren‘ (Golding, 2017). Ein weiteres solches Beispiel ist der Algorithmus von Google, der entscheidet, welche E-Mails in den ‚Posteingang‘ gelangen. Baldwin-Philippi et al. (2020) notieren, dass E-Mails bis heute einer der gängigsten Wege sind, Wahlberechtigte zu mobilisieren. Die Entscheidung, welche

Nachricht eine Person sieht, ist daher kritisch zu betrachten (Baldwin-Philippi et al., 2020). Hier ist zu erkennen, dass beim Mikrotargeting nicht nur die Inhalte der Werbeanzeigen relevant sind, sondern auch die Algorithmen der Plattformen, welche entscheiden, wie die Anzeige ausgeliefert wird. Eine weitere Studie zum ‚Ad-Delivery'-Algorithmus von Facebook hat ergeben, dass sowohl das Budget der Werbetreibenden als auch der Inhalt der Anzeige maßgeblich zum Algorithmus der Anzeigenbereitstellung von Facebook beitragen (Ali, 2019).

3.2.3 Öffentlichkeit

Die Risiken von Mikrotargeting in Zusammenhang mit der Öffentlichkeit sind zahlreich. Eine negative Auswirkung entsteht, wenn bestimmte Gruppen von Wahlberechtigten ignoriert werden, da sie nicht als ‚wertvoll' erachtet werden. Dies können beispielsweise Menschen sein, die nicht regelmäßig wählen (Dobber et al., 2017). So definieren einige Werbetreibende, die Geotargeting anbieten, bestimmte Regionen als ‚hochwertig' und messen anderen einen ‚niedrigen Wert' bei (Bashyakarla et al., 2019). Die betroffenen Gruppen von Wahlberechtigten werden somit aus dem politischen Diskurs ausgeschlossen. Auch werden sie nicht über die Kampagnen informiert und sind folglich unterrepräsentiert (Zuiderveen Borgesius et al., 2018). Im negativsten Fall kann dies zu einem ‚Defekt' des demokratischen Diskurses führen (Kruschinski und Haller, 2017, S. 17).

Mikrotargeting segmentiert die Wählerschaft in kleine Gruppen, um diesen die für sie relevantesten Themen zu liefern. Dies führt nach Bayer zur Fragmentierung der Öffentlichkeit, was dem demokratischen Prozess schadet (Bayer, 2020). Fragmentierung kann durch Mikrotargeting entstehen, indem die Öffentlichkeit den Überblick über allgemeine Themen verliert und sich ausschließlich auf interessenbezogene Inhalte konzentriert (Zuiderveen Borgesius et al., 2018). Diese Fragmentierung kann zusätzlich dazu führen, dass Menschen, die in der Politik tätig sind, unterschiedlichen Gruppen unterschiedliche Versprechen machen. Somit wird es schwierig, politische Parteien beziehungsweise ihre Repräsentanten für ihre Wahlversprechen zur Rechenschaft zu ziehen (Leerssen, 2019).

Polarisierung wird ebenfalls als eine negative Auswirkung von Mikrotargeting gesehen (Lewandowsky et al., 2020). Der Europäische Datenschutzausschuss (EDSA) bemerkt, dass es durch Mikrotargeting zu Filterblasen kommen kann, in denen Wahlberechtigte wiederholt mit den gleichen Informationen konfrontiert werden und in

zunehmend geringerem Maße unterschiedlichen Meinungen begegnen (Europian Data Protection Board,2018). Dies führt zu einer wachsenden ideologischen und politischen Polarisierung. Außerdem werden dadurch Betroffene für Falschinformationen anfälliger.

Die Risiken, die sich für die Demokratie durch den Einsatz von Mikrotargeting im Wahlkampf ergeben, sind somit vielfältig. Im folgenden Kapitel wird die Regulierung dieses Instruments diskutiert, in Bezug auf die Begrenzung der negativen Auswirkungen.

4. Regulierung von politischem Mikrotargeting

Der Bedarf an einer Regulierung von Mikrotargeting im politischen Wahlkampf ist größtenteils abhängig davon, welche Chancen und Risiken sich für die beteiligten Akteurinnen und Akteure und den gesamtgesellschaftlichen demokratischen Prozess ergeben. Das Zusammenspiel aus sozialen, politischen, rechtlichen und technischen Faktoren erschwert die Regulierung. Im vorherigen Kapitel haben wir die Chancen und Risiken kennengelernt, jedoch sind die Auswirkungen von Mikrotargeting bislang nicht ausreichend untersucht worden. Somit wird es schwer, die Auswirkungen der Regulierungen vorherzusagen.

Die Meinungen, ob und in welcher Form eine Regulierung stattfinden soll, sind gespalten. Zuiderveen Borgesius et al. behaupten, dass die Risiken durch Mikrotargeting für die Demokratie insbesondere im Europäischen Kontext geringfügig sind (Zuiderveen Borgesius et al., 2018). Auf der anderen Seite gibt es Vertreter, die für ein Mikrotargeting-Verbot stehen. Das Europäische Parlament ist der Ansicht, dass eine Profilerstellung für politische und wahlbezogene Zwecke sowie die Profilerstellung auf der Grundlage von Online-Verhalten, die die politischen Präferenzen einer offenbaren kann, verboten werden sollte (Europian Paralament, 2018, Point 9). Die Profilerstellung aus sozioökonomischer oder demografischer Art von Daten sollte ihrer Meinung nach auch verboten werden (Europian Paralament, 2018, Point 9). Ähnlich argumentieren Bennett und Oduro-Marfo (2019), die ist Privatsphäre eine essenzielle Voraussetzung für die politische Partizipation und somit sind Privatsphäre verletzende Mikrotargeting Methoden nicht akzeptabel.

Jedoch könnte ein Verbot von politischem Mikrotargeting auch negative Auswirkungen haben. Papakyriakopoulos et al. (2017) argumentieren, dass Mikrotargeting als eine

Verpflichtung der Parteien gesehen werden kann, da es zur politischen Willensbildung beiträgt. Ein Verbot von Mikrotargeting könnte schädlich für die Demokratie sein, denn es begrenzt die Möglichkeiten für politische Parteien, die Öffentlichkeit zu erreichen (Baldwin-Philippi et al., 2020). Das Verbot kann sich somit auf kleinere politische Parteien mit geringeren Geldern nachteilig auswirken, da Mikrotargeting eine kostengünstige Möglichkeit ist die Wählerschaft zu erreichen (Baldwin-Philippi et al., 2020).

Fernerhin könnte ein Verbot von Mikrotargeting zu einer Einschränkung des Rechtes der Meinungsfreiheit der politischen Parteien führen (Brkan, 2020). Da der politische Wahlkampf zum Recht des politischen Akteures gehört, sich auszudrücken, muss politisches Mikrotargeting reguliert werden, ohne dieses Recht zu verletzen. Auch Bayer (2020) nimmt mit dem Bezug auf den Fall vom Animals Defenders diese Problematik auf und weist darauf hin, dass mit eng bestimmten Regeln Mikrotargeting eingeschränkt werden kann, ohne das oben genannte Recht zu verletzten.

Durch ein Verbot von politischem Mikrotargeting könnten sich weitere Probleme ergeben. Erstens könnte eine unklare Definition von allgemeiner und gezielter politischer Werbung die Anwendung des Verbots erschweren (Brkan, 2020). Zweitens könnte dies dazu führen, dass politische Parteien ihre Mikrotargeting-Methoden verheimlichen und gezielte Werbung als allgemeine darstellen (Brkan, 2020).

In erster Linie konzentrieren sich die Regulierungsvorschläge und Maßnahmen auf einen besseren Schutz der Daten der Bürgerinnen und Bürger. Mikrotargeting benötigt große Mengen an personenbezogenen Daten, um effizient zu funktionieren. Als zweite Richtlinie wird ein höheres Maß an Transparenz gefordert. Dabei sollen Werbedienste von großen Plattformen transparenter gestaltet werden. Außerdem soll daraus die Rechenschaftspflicht von politischen Akteuren und sozialen Plattformen ermittelt und erhöht werden.

In diesem Kapitel werden wir auf alle diese Bemerkungen näher eingehen. Der Fokus wird auf die Maßnahmen, die die Europäische Union getroffen hat, legen. Außerdem werde ich zusammenfassen, wie große Plattformen wie Facebook und Google im Laufe der letzten Jahre ihre Targeting-Optionen für den politischen Wahlkampf verändert haben.

4.1 DSGVO im Kontext des politischen Wahlkampfs

Eine der Eigenschaften, die Mikrotargeting ausmacht, ist, große Mengen an persönlichen Daten zu sammeln und zu verarbeiten, um dann die personalisierten Werbebotschaften zu erstellen. Viele der Risiken, die durch die Anwendung von Mikrotargeting entstehen können, stammen aus dieser Eigenschaft. Datenschutzgesetze spielen daher eine wichtige Rolle bei den Regulierungen der Sammlung und Verarbeitung von personenbezogenen Daten.

In der Europäischen Union gilt seit Mai 2018 die Datenschutzgrundverordnung (im Folgenden DSGVO). Im Kontext vom Mikrotargeting im politischen Wahlkampf sind die folgenden Artikel der DSGVO von Interesse.

4.1.1 Persönliche Daten sammeln

Die DSGVO definiert als personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ (Artikel 4.1, DSGVO). Unter diese Informationen können unter anderem Daten über den Standort der Person, aber auch psychische, wirtschaftliche und soziale Merkmale fallen (Art. 4.1, DSGVO). Solche Informationen sind essenziell für die Durchführung von Mikrotargeting. Die Sammlung von persönlichen Daten ist nicht allgemein erlaubt. Das Sammeln und Speichern von Daten ist in der Definition von *Verarbeitung* in der DSGVO inbegriffen (Art. 4.2, DSGVO). In Artikel 5 werden die Grundsätze für die Verarbeitung personenbezogener Daten festgelegt. Nach Artikel 5 gilt insbesondere: Die erhobenen Daten dürfen nur für „festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“ (Art. 5.1.b, DSGVO). Zusätzlich sollten sie nach Artikel 5 „in einer auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.“ (Art. 5.2.a, DSGVO). Dieser Absatz insbesondere ist schwer im Kontext von Mikrotargeting durchzusetzen, weil die Prozesse sehr unübersichtlich sind.

Außerdem legt Artikel 9 fest, wann Daten aus besonderen Kategorien verarbeitet werden können. Darunter fallen unter anderem Daten wie ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Artikel 9.1, DSGVO). Diese Art von Daten können zum Beispiel verarbeitet werden, wenn eine

rechtmäßige Einwilligung der betroffenen Person gegeben ist (Art. 9.2.a, DSGVO) oder wenn die Person selbst diese Daten öffentlich gemacht hat (Art. 9.2.e, DSGVO).

Die Bedingungen für die Rechtmäßigkeit der Verarbeitung von Daten werden im Artikel 6 der DSGVO beschrieben. Nach dem Leitfaden der Kommission (2018) werden während der Wahlen dazu folgende Gründe rechtmäßig: die Einwilligung einer Person (Art. 6.1.a., DSGVO), die Erfüllung einer rechtlichen Verpflichtung (Art. 6.1.c, DSGVO), die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt (Art. 6.1.e, DSGVO) und das berechtigte Interesse eines der Akteure (Art. 6.1.f, DSGVO). Der Europäische Datenschutzausschuss hat Ende Oktober 2020 weitere Richtlinien für die gezielte Ansprache von Sozial-Media-Nutzern veröffentlicht. In diesen Richtlinien werden nur zwei Rechtsgrundlagen anerkannt, die die Verarbeitung von Daten für Mikrotargeting in sozialen Medien rechtfertigen könnten: die Einwilligung der betroffenen Person oder berechtigte Interessen (Europian Data Protection Board, 8/2020).

Die gängige Form, rechtmäßig Daten zu verarbeiten, ist durch die Einwilligung der Person. In Artikel 7 (DSGVO) werden die Bedingungen, anhand derer eine legitime Einwilligung eingeholt werden kann, erläutert. Die EDSA hat weitere Leitlinien im Jahr 2020 vorgestellt, darunter, dass freiwillige Einwilligung bedeutet, dass die Person die echte Wahl und die Kontrolle hat (EDSA, 05/2020).

Dies ist insbesondere deshalb wichtig, da oft eine Einwilligung einfache zu bekommen trotz der vielen Reglungen (Dobber et al., 2017). Viele Webseiten verwenden *Consent Management Platforms*, die in die Benutzeroberfläche eingebettet sind, um eine rechtliche Grundlage zum Sammeln und Verarbeiten von personenbezogenen Daten zu schaffen. Studien haben jedoch gezeigt, dass dabei oft *Dark Patterns* eingesetzt werden (Soe et al., 2020; Nouwens et al., 2020; zur automatischen Erkennung von Dark Patterns Hausner, 2021). *Dark Patterns* sind Schnittstellendesigns, mit deren Hilfe versucht wird, den Endbenutzer durch bestimmte Punkte manipulativ zum gewünschten Verhalten zu führen (Datenethikkommission, 2019). In diesem Kontext sind solche Designs zum Beispiel vormarkierte Einstellungen bei der Annahme aller Tracking-Technologien einer bestimmten Webseite. Solche Praktiken verstoßen gegen die DSGVO.

Komplementär zur DSGVO gibt es auch die Datenschutzrichtlinie für elektronische Kommunikation (2002) die weiteren Regelungen für Tracking-Technologien beinhaltet.

Grundsätzlich wird auch hier eine informierte Einwilligung der betroffenen Person für den Einsatz von Tracking-Technologien beschrieben. Insbesondere sollen die Nutzer über die Zwecke der Verarbeitung informiert werden (Art. 5.3, Richtlinie 2002/58/EG). Die Europäische Kommission hat im Jahr 2017 Vorschläge zur Verbesserung der Richtlinie veröffentlicht. Im Jahr 2021 haben sich die Mitgliedstaaten auf ein Verhandlungsmandat für die überarbeitete Richtlinie zum E-Datenschutz geeinigt. Dabei werden weitere besondere Aspekte angesprochen, wie der Umgang mit „elektronischen Kommunikationsmetadaten“ und den „Inhalten von elektronischen Kommunikationen“ (Art. 4.3.b, c für Definition, Art. 5–11 für den Umgang mit dieser Art von Daten, European Union, 2021).

4.1.1 Profiling und Targeting

Um Mikrotargeting durchführen zu können, werden Daten nach deren Sammlung weiterverarbeitet, um personalisierte Profile zu erstellen, anhand derer später die gezielte Kommunikation stattfinden wird. Profiling ist in der DSVO allgemein nicht verboten und wird wie folgt definiert:

„jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“ (Artikel 4.4, DSGVO).

Die EDSA sieht in ihrer Erklärung zur Verwendung personenbezogener Daten im Rahmen politischer Kampagnen solche Datenverarbeitungstechniken als ein erhebliches Risiko nicht nur für das Recht auf Privatsphäre und Datenschutz, sondern auch für den demokratischen Prozess (EDSA, 2019). Eine weitere Bemerkung ist, dass durch solche Prozesse Rückschlüsse auf eine persönliche Kategorie von Daten gezogen werden können, zum Beispiel die politischen Meinungen einer Person. Jedoch müssen die Bedingungen von Artikel 9 (DSGVO) auch in diesem Fall erfüllt sein (EDSA, 2019).

Die EDSA hat im Jahr 2020 eine Richtlinie zu Targeting in sozialen Medien vorgestellt. Das ist die erste Richtlinie, die sich näher mit Mikrotargeting befasst. In der Praxis ist

es oft schwierig ist die rechtlichen Rollen und Verantwortlichkeiten an den beteiligten Akteuren zuzuweisen. Deswegen hat die EDSA anhand des folgendes Targeting Modells die Entscheidung zur Rollenverteilung bestimmt. Es werden drei Arten von Targeting-Methoden beschrieben, nämlich Targeting (Europian Data Protection Board, 08/2020, Paragraf 40, S.13)

1. auf Basis bereitgestellter Daten, wie Alter und Geschlecht der Nutzerinnen und Nutzer.
2. auf Basis beobachteter Daten. Diese Daten beschreiben das Verhalten der Nutzerinnen und Nutzer auf den sozialen Plattformen.
3. auf Basis von abgeleiteten Daten. In diesem Fall können Informationen aus dem Verhalten der Nutzerinnen und Nutzer abgeleitet werden.[4]

Außerdem wird in dem Leitfaden der Kommission zur Anwendung des EU-Datenschutzrechts im Zusammenhang mit Wahlen dargestellt, dass politische Parteien und Stiftungen, Informationsbroker und Anbieter von Datenanalysen auch als online Werbeanbieter eine Datenschutz-Folgenabschätzung durchführen müssen (Kommission, 2018).

Die DSGVO ist also ein wichtiges Instrument für die Regulierung von politischem Mikrotargeting in politischen Wahlkampagnen. Es ist jedoch noch nicht klar, inwiefern dadurch die negativen Auswirkungen von Mikrotargeting eingedämmt werden (Europian Comission, 2020a). Obwohl die DSGVO dazu geführt hat, dass Mikrotargeting nicht im gleichen Grad wie in den USA angewendet wird (Dobber, 2019a).

4.2 Verhaltenskodex zur Bekämpfung von Desinformation

Eine Initiative der Europäischen Union ist die Einführung eines Verhaltenskodexes zur Bekämpfung von Desinformation im April 2018. Dabei handelt es sich um einen freiwilligen selbstregulierenden Verhaltenskodex, der von Vertretern von Online-Plattformen, Werbetreibenden, der Werbebranche und führenden sozialen Plattformen befolgt wird, um die Verbreitung von Online-Desinformation und Fake News zu

4 Eigene Übersetzung aus dem Englischen

minimieren (Comission,2018). Ein von der Kommission genanntes Ziel dessen ist die Förderung der Transparenz in der politischen Werbung (Paragraf I.iii, Comission,2018). Dies soll unter anderem mittels Indikatoren für Vertrauenswürdigkeit der Informationsquellen und Transparenz in Bezug auf Medieneigentum und überprüften Identitäten erfolgen (Paragraf I.viii, Comission, 2018). Nach dem Selbstregulierungskodex haben sich die Unterzeichnenden auch dazu verpflichtet, politische Anzeigen eindeutig als gesponserte Inhalte zu kennzeichnen und die tatsächliche Identität des Sponsors zu offenbaren (Paragraf II.B, Comission, 2018). Es handelt sich somit um eine relevante Maßnahme zur Regulierung von Mikrotargeting im politischen Wahlkampf.

Facebook, Google, Twitter und Mozilla sowie Werbetreibende und Teile der Werbebranche haben den Kodex im Oktober 2018 unterschrieben. Microsoft und TikTok zählen ebenfalls dazu (Comission,2018). Im Jahr 2021 planen weitere Unternehmen beizutreten, darunter solche mit Expertenwissen und technischen Lösungen wie WhoTargetsMe, Avaaz und Globsec (Comission, 2021a).

Im Folgenden werden einige der Selbstregulierungsmaßnahmen der führenden sozialen Netzwerke wie Facebook, Google und Twitter betrachtet.

4.2.1 Beispiele zur Selbstregulierung der Plattformen

Die großen Technologiekonzerne wie Facebook und Google zählen zu den Hauptakteuren beim Phänomen des politischen Mikrotargeting. In jeder Wahlperiode werden beträchtliche Summen für politische Onlinewerbung ausgeben. Zurzeit, während einer Pandemie, scheint ihre Bedeutung noch zugenommen zu haben. Unter anderem hat der Verhaltenskodex für Desinformation dazu geführt, dass die führenden Online-Plattformen Veränderungen bei ihren Geschäftsmodellen und -bedingungen vorgenommen haben.

Die Einführung von Werbearchiven ist eines der effektivsten Werkzeuge, um Transparenz in der politischen Werbung zu erzeugen. Diese Werbebibliotheken speichern außer den aktuellen Werbeanzeigen und deren Sponsoren auch weitere Informationen. Zum Beispiel werden in der Werbebibliothek von Facebook zusätzlich die Reichweite (wie oft die Anzeige gesehen wurde), die Kosten, die demografischen Angaben und der Standort einer politischen Werbung gezeigt. Reichweite und Ausgaben werden nicht exakt dargestellt. Die Informationen werden außerdem für

sieben Jahre gespeichert. Außer den aktiven Werbeanzeigen kann auch unter inaktiven gesucht werden (Facebook,2021b), für Deutschland zum Beispiel ab April 2019 und in den USA ab Mai 2018. Ähnlich hat Google seine Werbebibliothek im März 2019 auch für Europa veröffentlicht. Zusätzlich können die Werbebibliotheken mit Anwendungsprogrammierschnittstellen (APIs) unterstützt werden, die einen direkten Kanal zum Extrahieren von Informationen bieten. Diese eignen sich optimal für die Erforschung der politischen Werbung in sozialen Medien.

Diese Werbearchive bieten eine Maßnahme gegen einige negative Auswirkungen, die im Kapitel 3.2 dargestellt sind. Politische Mikrotargeting-Werbeanzeigen werden somit zugänglich für die Öffentlichkeit. Die Inhalte der politischen Werbeanzeigen können dadurch nachverfolgt und überprüft werden. Somit kann auch Desinformation bekämpft werden.

Trotzdem gibt es noch technische Probleme bei den Werbebibliotheken. Edelson et al. (2020) haben während ihrer Sicherheitsanalyse unter anderem erkannt, dass zahlreiche Werbetreibende Anzeigen schalten können, ohne darzulegen, wer für diese bezahlt hat. Ferner gab es einen Ausfall der Werbebibliothek, der dazu führte, dass 40 % der Anzeigen nicht zugänglich waren (Edelson et al.,2020). Weiterhin sind Barett und Kreiss (2019) der Ansicht, dass die Werbearchive von Facebook nur das niedrigste Maß an Informationen bereitstellen und umfangreichere Angaben nötig sind, um weitere Forschung über politische Werbeanzeigen zu ermöglichen.

Außer den Werbebibliotheken werden auch Fact-Checking-Mechanismen eingesetzt, um zu überprüfen, ob eine Werbeanzeige wahr oder irreführend ist. Dabei werden oft maschinelle Lernalgorithmen eingesetzt, aber auch durch Drittanbieter erstellte Software (Lyons,2018). Solche Maßnahmen sollen gegen Desinformation auch im politischen Kontext wirksam sein.

Obwohl Facebook im Mittelpunkt des Cambridge-Analytica-Skandals stand, ist es das einzige Unternehmen, das politische Werbung mit der Möglichkeit erlaubt, unterschiedliche personenbezogene Eigenschaften der Nutzenden zu wählen (Facebook,2021c). Im Gegensatz dazu erlaubt Google für politische Werbung nur die Kriterien Standorte, demografische Merkmale und Kontext-Targeting, zum Beispiel Anzeigenplatzierung und Themen (Google, 2021a). Außerdem hat der Konzern in Kanada und Washington politische Werbung allgemein verboten. Dies geschah, weil laut Google der Aufwand zu hoch und es technisch nicht umsetzbar war, im

Zusammenspiel mit länderspezifischen Regulierungen und ‚Real-Time-Bidding' für Werbeanzeigen eine politische Werbung als solche zu identifizieren (Burkell, 2019). Twitter beschloss im Jahr 2019, keine Werbung mit politischen Inhalten mehr zu erlauben, weil „die Reichweite politischer Botschaften verdient, nicht gekauft werden soll" (Chester und Montgomery, 2019). Die Plattformen Microsoft (Microsoft, 2021), LinkedIn (LinkedIn, 2021) und TikTok (Chandlee, 2020) verbieten ebenfalls politische Werbeanzeigen.

Ausgenommen von den Werbebibliotheken gibt es anderes Werkzeug, das es Nutzenden erlaubt, den Mikrotargetingprozess besser zu verstehen. Es handelt sich um die Funktion ‚Warum sehe ich auf Facebook Anzeigen eines bestimmten Werbetreibenden?" (Facebook, 2021d). Hier wird den Nutzenden zusammengefasst erklärt, wie die Targeting-Funktionen anhand personenbezogener Daten bei Facebook funktionieren. Um ferner die ständige Überwachung der Nutzenden zu minimieren, entwickelte Mozilla Fox eine Facebook-Container-Erweiterung. Sie speichert die Identität der Nutzenden in einem separaten Container-Tab, was es Facebook erschwert, eine Person im Web außerhalb von Facebook zu verfolgen (Mozilla, 2021)

Die Kommission hebt weitere ‚Best Practice'-Beispiele hervor (Commission, 2021b)

4.2.2 Bewertung des bisherigen Kodexes

Der Verhaltenskodex wurde im vergangenen Jahr bewertet (Europian Commission, 2020b). Obwohl er ein effektives Instrument, unter anderem für Transparenz in der politischen Werbung ist, gibt es Probleme bei seiner Durchsetzung (Europian Commission, 2020b). Eine der von Forschenden genannten, aber auch aus der Bewertung der Kommission hervorgegangenen Schwierigkeiten ist, dass unterschiedliche Definitionen für den Begriff ‚politische Werbung' benutzt werden (Europian Commission, 2020b; Dobber et al., 2019). Dies kann die Erforschung der Effekte politischer Werbung erschweren. Außerdem wird es schwieriger, politische Werbetreibende zu identifizieren und ihren Einfluss im Kontext der Wahlen zu regulieren. Um eine Uniformität der Definitionen zu erreichen, wird eine gemeinsame regulative Herangehensweise gefordert.

Bei den Lücken, die der Verhaltenskodex nicht explizit behandelt, wird auch Mikrotargeting thematisiert. Außerdem wird trotz der von der Kommission anerkannten

Risiken für die Demokratie Mikrotargeting im Kontext des Wahlkampfes weiterhin nicht verboten oder explizit beschränkt (Europian Commission, 2020b).

Aufgrund der anerkannten Lücken hat die Europäische Kommission dieses Jahr beschlossen, weitere Schritte zur Verstärkung des Verhaltenskodexes einzuführen. In den Vorschlägen wird auch beschrieben, dass politische Werbung im Kontext der Wahlen durch den kommenden Europäischen Aktionsplan für die Demokratie und den Digital Service Act noch konkreter reguliert werden soll (Commission, 2021c).

Die Europäische Kommission hat zwischen Januar und Mai 2019 eine gezielte Überwachung der Umsetzung der Verpflichtungen durch Facebook, Google und Twitter mit besonderer Relevanz für die Integrität der Wahlen zum Europäischen Parlament durchgeführt. Es folgten eine Reihe von Selbstbewertung Berichte, die sogenannten *Transparency Reports* dieser drei Großkonzerne. Daraus geht hervor, dass sie umfassende Anstrengungen unternommen haben, um ihre Verpflichtungen umzusetzen.

4.3 Europäischer Aktionsplan für Demokratie

Der im Dezember 2020 veröffentlichte Europäische Aktionsplan für Demokratie hat drei Hauptziele (Kommision,2020d, S.3):

1. Schutz der Integrität von Wahlen und Förderung der demokratischen Teilhabe,
2. Stärkung der Medienfreiheit und des Medienpluralismus,
3. Bekämpfung von Desinformation.

Dieser Aktionsplan benennt die Risiken, die durch den Einsatz von Mikrotargeting im Wahlkampf für die Demokratie sich ergeben können als Ursache der Forderung weiterer Maßnahmen. Es wird des Weiteren erkannt das neue Techniken zu dieser gezielten Ansprache der Wählerschaft geführt hat. Und es soll noch eine strengere Regulierung von Mikrotargeting und psychologisches Profiling stattfinden. Dafür werden weitere Transparenz Maßnahmen gefordert, wie Kennzeichnungspflichten der gesponsorten Inhalte. (Kommission, 2020d)

4.4 EU-Digital-Service-Act

Der geplante Digital-Service-Act soll online Dienste und Online-Plattformen weiter regulieren (Kommission, 2021). Auch hier wird Mikrotargeting als Risiko erkannt

insbesondere seine Anwendung in online Plattformen, die durch ihre Architekturen Effekte maximieren (Paragraf 43,46, Commission,2020). Trotz der Benennung der Risiken wird auch kurz erwähnt, dass keine Beweise für die Beeinflussung der Wählende gibt (46, Commission,2020). Durch das Digital-Service-Act sollen online-Werbungen besser reguliert werden. Insbesondere in Bezug auf die politische Werbung sollen mehr Informationen zugänglich gemacht werden, wie zum Beispiel der Werbebetreiber oder die Werbekosten und dabei sollen diese Informationen ich Echtzeit erreichbar sein (Commission,2020).

4.5 Zusammenfassung EU-Regulierung

Die Europäische Union erkennt die Risiken vom politischen Mikrotargeting auf die Demokratie und fordert weitere Maßnahmen für seine Regulierung. Die DSGVO bietet zusammen mit den neuen Richtlinien für E-Datenschutz, Targeting in sozialen Medien und der Verstärkung von Verhalten Kodes ein starkes Instrument gegen die negativen Auswirkungen von Mikrotargeting. Viele der Bedenken hinsichtlich der Überwachung von Mikrotargeting haben eine Regelung gefunden. Jedoch ist die Durchsetzung von DSGVO und Verhaltenskodex nicht einfach und benötigt weitere Unterstützung von den europäischen Ländern (Commission,2020a) und Plattformen (Commission, 2021c) Die informierte Einwilligung ist immer noch eine Problematik sowohl als auch die technischen Probleme der Plattformen, neue Maßnahmen einzusetzen. Einige Maßnahmen wie die ad Bibliotheken, die eine neue Welle an Forschung des Mikrotargeting auch in Europa gebracht haben, schaffen die Voraussetzung, um die Auswirkungen des politischen Mikrotargetings im Wahlkampf zu verstehen.

5. Zusammenfassung und Ausblick

Ziel dieser Masterarbeit war es, mögliche Auswirkungen von Big Data auf die Demokratie am Beispiel von politischem Wahlkampf darzustellen. Um dies zu erzielen wurden Quellen hauptsächlich aus der Politikwissenschaft, jedoch auch aus der Datenwissenschaft und Sozialwissenschaft untersucht. Daraus haben sich folgende Erkenntnisse gebildet.

Wahlkampf, welcher durch Big Data Anwendungen unterstützt wird, nennt sich in der Literatur oft datenbasierender Wahlkampf. Des Weiteren wurde erkannt, dass in der Literatur der datenbasierende Wahlkampf oft mit der Nutzung von politischem Mikrotargeting eingeht. Das Phänomen von Mikrotargeting ist recht neu in Europa. Um

die Literatur weiter zu untersuchen wurde der Fokus auf die Auswirkungen von Mikrotargeting auf die Demokratie gesetzt. Die Auswirkungen von Mikrotargeting können einerseits Chancen für die Demokratie bieten und andererseits Risiken darstellen.

Die Chancen bestehen aus einer erhöhten Partizipation der Bürgerinnen und Bürger, einer besseren Repräsentation der Wählerinnen und Wähler und zuletzt einer Bereicherung des öffentlichen politischen Diskurses. Dagegen bestehen bei Mikrotargeting Risiken der Verletzung der Privatsphäre, der Manipulation der Bürgerinnen und Bürger, Fragmentierung und Polarisierung der Öffentlichkeit, sowie der Opazität der Prozesse und Ziele der politischen Akteure.

Zunächst wurde die Verminderung der Risiken mit neuen Regelungen durch die Europäischen Union dargestellt. Viele der Risiken werden als Bedrohung der Demokratie betrachtet und entsprechend wurden erste Versuche gemacht, um Mikrotargeting zu regulieren. Auch Veränderungen der Geschäftsbedingungen von Plattformen wie Facebook wurden dargestellt. Diese Maßnahmen führen zu einer Verbesserung der Lage. Durch die Einführung von Werbebibliotheken können die Inhalte der Werbungen besser untersucht werden. Durch die Automatisierung der Generierung und des Verkaufs der Werbeanzeigen online ist die Überwachung dieser Prozesse jedoch schwer. Dabei könnten allerdings technische Lösungen helfen.

Durch den Einsatz von Mikrotargeting im Wahlkampf werden immer mehr technische Elemente Teil des demokratischen Prozesses. Einerseits wird Mikrotargeting hauptsächlich in den sozialen Medien betrieben, wo die Technikgestaltung in der Verantwortung dieser großen Konzerne liegt. Andererseits spielen auch weitere kleinere technische Firmen, die sich auf Werbetechnologien spezialisiert haben, eine zunehmende Rolle dabei, politische Akteure zu unterstützen. Bei der Entwicklung der digitalen Technologien, die beim Mikrotargeting eingesetzt werden müssen, also auch immer die Auswirkungen auf die Demokratie mitbetrachtet werden.

Eine interdisziplinärer Forschungsansatz aus den Disziplinen Informations-, Daten-, Sozial-, Kommunikations-, Rechts-, Politik- und Medienwissenschaft wird benötigt, um die Effekte und Prozesse von Mikrotargeting weiter zu verstehen. Weiterhin wird ein größeres Maß an Transparenz von den Onlinekonzernen benötigt, um das Phänomen verstehen und effizient regulieren zu können.

Literaturverzeichnis

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A., & Rieke, A. (2019). Discrimination through optimization: How Facebook's Ad delivery can lead to biased outcomes. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1-30.

Baldwin-Philippi, J. (2019). Data campaigning: Between empirics and assumptions. Internet Policy Review, 8(4), 1-18. DOI: 10.14763/2019.4.1437.

Baldwin-Philippi, J., Bode, L., Sheingate, A., & Kreiss, D. (2020). Digital political Ethics: aligning principles with practice. Center for Information, Technology, and Public Life. https://citapdigitalpolitics.com/wp-content/uploads/2020/01/Jan-8-FINAL-Digital-Political-Campaigning-Report-2020-FINAL-1.pdf.

Barrett, B., & Kreiss, D. (2019). Platform transience: changes in Facebook's policies, procedures, and affordances in global electoral politics. Internet Policy Review, 8(4), 1-22.

Barrett, B., Kreiss, D., Fox, A. & Ekstrand, T. (2020). Political Advertising onPlatforms in the United States:A Brief Primer. https://citapdigitalpolitics.co,et al.m/wp-content/uploads/2020/01/PlatformAdvertisingPrimer_CITAP.pdf

Bashyakarla, V., Hankey, S., Macintyre, A., Renno, R., & Wright, G. (2019). Personal Data: Political PersuasionInside the Influence Industry. How It Works. Data and Politics Team. Tactical Technology Collective, March.

Bayer, J. (2020). Double harm to voters: Data-driven micro-targeting and democratic public discourse. Internet Policy Review, 9(1), 1-17. DOI: 10.14763/2020.1.1460.

Bennett, C., & Gordon, J. (2020). Understanding the “Micro” in Micro-Targeting: An Analysis of Facebook Digital Advertising in the 2019 Federal Canadian Election. Available at SSRN 3589687 or http://dx.doi.org/10.2139/ssrn.3589687

Bennett, C., & Oduro Marfo, S. (2019, October). Privacy, voter surveillance and democratic engagement: challenges for data protection authorities. In International Conference of Data Protection and Privacy Commissioners (ICDPPC). DOI: 10.2139/ssrn.3517889

Bennett, Colin J. 2018. “Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as They Do in North America?” International Data Privacy Law 6 (4): 15

Bodó, B. & Helberger, N. & de Vreese, C. H. (2017). Political micro-targeting: a Manchurian candidate or just a dark horse?. Internet Policy Review, 6(4). https://doi.org/10.14763/2017.4.776

Boyd, D., & Crawford, K. (2012). Critical Questions for Big Data in Information„Communication & Society”. Communication and Society, 15(5), 662-679. DOI: 10.1080/1369118X.2012.678878.

Brkan, M. (2020). EU fundamental rights and democracy implications of data-driven political campaigns. Maastricht Journal of European and Comparative Law, 27(6), 774-790. DOI: 10.1177/1023263X20982960.

Burkell, J. & Regan, P. M. (2019). Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy. Internet Policy Review, 8(4). https://doi.org/10.14763/2019.4.1438

Cadwalladr, C. (2017). The great British Brexit robbery: how our democracy was hijacked. The Guardian, 7. https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The guardian, 17, 22 Letzter Zugriff 18.10.2021 https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-

Chandlee, B. (2020). Richtlinien für Werbeanzeigen auf TikTok. tiktok.com. Letzter Zugriff 18.10.2021, von https://newsroom.tiktok.com/de-de/richtlinien-fur-werbeanzeigen-auf-tiktok

Chester, J. & Montgomery, K. C. (2017). The role of digital marketing in political campaigns. Internet Policy Review, 6(4). DOI: 10.14763/2017.4.773

Chester, J., & Montgomery, K. C. (2019). The digital commercialisation of US politics—2020 and beyond. Internet Policy Review, 8(4), 1-23. https://doi.org/10.14763/2019.4.1443

Comission (2018). EU Code of Practice on Disinformation https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

Comission (2021a). Code of Practice on disinformation: Commission welcomes new prospective signatories and calls for strong and timely revision https://ec.europa.eu/commission/presscorner/detail/en/IP_21_4945

Commission (2020). COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020SC0348&rid=1

Commission (2021b). 'Code of Practice on Disinformation: Annex II: Current best practices from Signatories of the code of Practice https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

Commission (2021c). European Commission Guidance on Strengthening the Code of Practice on Disinformation https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585

Commission, (2020a). Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264

Datenethikkommission. (2019, Oktober). Gutachten der Datenethikkommission. Datenethikkommission der Bundesregierung Bundesministerium des Innern, für Bau und Heimat. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6

Datenschutz-Grundverordnung DSGVO: als übersichtliche Seite. Datenschutz-Grundverordnung (DSGVO). https://dsgvo-gesetz.de/ (letzter Zugriff 18.10.21)

Dobber, T., & Fathaigh, Ó. R., & Zuiderveen Borgesius, FJ (2019a). The regulation of online political micro-targeting in Europe. Internet Policy Review, 8(4). DOI: 10.14763/2019.4.1440.

Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. (2019b). Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns. new media & society, 21(6), 1212-1231.

Dobber, T., Trilling, D., Helberger, N., & De Vreese, C. H. (2017). Two crates of beer and 40 pizzas: the adoption of innovative political behavioural targeting techniques. Internet Policy Review, 6(4), 1-25. DOI: 10.14763/2017.4.777.

Edelson, L, Lauinger, T., McCoy, D (2020): Security Analysis Of The Facebook Ad Library.

EDSA (2019) Erklärung Nr. 2/2019 zur Verwendung personenbezogener Daten im Rahmen politischer Kampagnen. https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-03-13-statement-on-elections_de.pdf

EDSA, (05/2020) Leitlinien zur Einwilligung gemäß Verordnung 2016/679 Version 1.1 angenommen am 4. Mai 2020, (letzter Zugriff 18.10.21)

Europäisches Parlament (2002) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation). (2002, 31. Juli). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&from=DE

European Commission (2020a): “Commission Staff Working Document: Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement” Verfügbar unter: https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement

European Commission. (2020b). Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation. eur-lex.europa.eu. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264

European Parliament (2018) resolution of 25 October 2018 on the use of Facebook users’ data by Cambridge Analytica and the impact on data protection

(2018/2855(RSP)), Point 9 https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_EN.html (letzter Zugriff 18.10.21)

European Union (2021). Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)-Mandate for negotiations with EP. (2021, 10. Februar). https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

Europian Data Protection Board. (8/2020). Adopted on 2021, 13. April.Guidelines 8/2020 on the targeting of social media users. edpb.europa.eu. https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

Facebook (2012a). Wie Lookalike Audiences funktionieren. Letzter Zugriff 18.10.2021, von https://de-de.facebook.com/business/help/1108247545961158?id=401668390442328&helpref=search&sr=7&query=lookalike

Facebook (2021e) Dynamische Anzeigengestaltung. Letzter Zugriff 18.10.2021, von https://de-de.facebook.com/business/help/170372403538781

Facebook. (2021b). What is the Facebook Ad Library and how do I search it? Letzter Zugriff 18.10.2021, von https://www.facebook.com/help/259468828226154/?helpref=related

Facebook. (2021c). How does Facebook decide which ads to show me? facebook.com/help. Letzter Zugriff 18.10.2021, von https://www.facebook.com/help/562973647153813?helpref=about_content

Facebook (2021d). Why am I seeing ads from an advertiser on Facebook? facebook.com. Letzter Zugriff 18.10.2021, von https://www.facebook.com/help/794535777607370

Facebook. (29. Juli, 2021). Anzahl der monatlich aktiven Facebook Nutzer weltweit vom 1. Quartal 2009 bis zum 2. Quartal 2021 (in Millionen) [Graph]. In Statista. Zugriff am 19. Oktober 2021, von

https://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/

Fanta, A. (2019). Eu-Parlament teilte Wählerdaten mit umstrittener Firman die auch für Trump und Brexit arbeitete. https://netzpolitik.org/2019/eu-parlament-teilte-waehlerdaten-mit-umstrittener-firma-die-auch-fuer-trump-und-brexit-arbeitete/a

Golding, D. (2017, 15. September). Facebook Moves to Prevent Advertisers From Targeting Haters. ProPublica. https://www.propublica.org/article/facebook-moves-to-prevent-advertisers-from-targeting-haters

Google (2021a). Political content Letzter Zugriff 18.10.2021, von https://support.google.com/adspolicy/answer/6014595?hl=en

Gorton, W. A. (2016). Manipulating citizens: How political campaigns' use of behavioral social science harms democracy. New Political Science, 38(1), 61-80.

Hausner. and Gertz, M. 2021. Dark Patterns in the Interaction with Cookie Banners. Position Paper at the Workshop "What Can CHI Do About Dark Patterns?" at the CHI Conference on Human Factors in Computing Systems, May 8-13, 2021, Yokohama, Japan.5 pages. https://dbs.ifi.uni-heidelberg.de/files/Team/phausner/publications/Hausner_Gertz_CHI2021.pdf

Hegelich, S. & Medina Serrano, J. C. (2019, Oktober). MICROTARGETINGIN DEUTSCHLAND BEI DER EUROPAWAHL 2019. medienanstalt-nrw.de.

Hellweg, E. (2012). The first big data election. Harvard Business Review, 13.

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf

Kommission Leitfaden (2018) Leitfaden der Kommission zur Anwendung des EU-Datenschutzrechts im Zusammenhang mit Wahlen Ein Beitrag der Europäischen Kommission zum Treffen der Führungsspitzen in Salzburg am 19./20. September 2018. (2018, 12. September). eur-lex.europa.eu. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52018DC0638

Kommission, (2020) Digital Service Act. Verfügbar unter: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-

services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_en

Kommission. (2020d). Mitteilung der Kommission an das Europäische Parlament , den, Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0790&from=EN

Kreiss D. (2012). "Yes we can Profile you" https://www.stanfordlawreview.org/online/privacy-paradox-yes-we-can-profile-you/

Kreiss, D. (2016). Prototype politics: Technology-intensive campaigning and the data of democracy. Oxford University Press.

Kreiss, D., & McGregor, S.C. (2018). Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle. Political Communication, 35, 155 - 177.

Krotzek, L. J. (2019). Inside the voter's mind: the effect of psychometric microtargeting on feelings toward and propensity to vote for a candidate. International Journal of Communication, 13, 21.

Kruschinski, S., & Haller, A. (2017). Restrictions on data-driven political micro-targeting in Germany. Internet Policy Review, 6(4), 1-23. DOI: 10.14763/2017.4.780.

Laney, D. (2001). 3D data management: Controlling data volume, velocity and variety. META group research note, 6(70), 1.

Lavigne, M. (2020). Strengthening ties: The influence of microtargeting on partisan attitudes and the vote. Party Politics, 1354068820918387. DOI: 10.1177/1354068820918387.

Leerssen, P., Ausloos, J., Zarouali, B., Helberger, N., & de Vreese, C. H. (2018). Platform ad archives: Promises and pitfalls. Internet Policy Review, 8(4).

Lewandowsky, S., Smillie, L., Garcia, D., Hertwig, R., Weatherall, J., Egidy, S., ... & Leiser, M. (2020). Technology and democracy: Understanding the influence of online technologies on political behaviour and decision-making.

LinkedI. (2021). LinkedIn Advertising Policies. linkedIn.com. Letzter Zugriff 18.10.2021, von https://www.linkedin.com/legal/ads-policy#4

Lyons, T. (2018, 14. Juni). Hard Questions: How Is Facebook's Fact-Checking Program Working? about.fb.com. http://about.fb.com/news/2018/06/hard-questions-fact-checking/

Macintyre, A. (2021,8.April). The Influence Industry Long List: The Business of Your Data and Your Vote, tacticaltech.org. https://ourdataourselves.tacticaltech.org/posts/the-influence-industry-long-limst/l

Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. Proceedings of the national academy of sciences, 114(48), 12714-12719.

Medina Serrano, J. C., Papakyriakopoulos, O., & Hegelich, S. (2020). Exploring political ad libraries for online advertising transparency: lessons from Germany and the 2019 European elections. In International conference on social media and society (pp. 111-121).

Microsoft. (2021). Disallowed content policies. microsoft.com., von Letzter Zugriff 18.10.2021 von https://about.ads.microsoft.com/en-us/resources/policies/disallowed-content-policies

Mozilla (2021).Facebook. Well contained. Keep the rest of your life to yourself. mozilla.org/. Letzter Zugriff 18.10.2021, von https://www.mozilla.org/en-US/firefox/facebookcontainer/

Nickerson, D. W., & Rogers, T. (2014). Political campaigns and big data. Journal of Economic Perspectives, 28(2), 51-74.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the 2020 CHI conference on human factors in computing systems (pp. 1-13).

Ortega, A. L. (2020, June 10). Are microtargeted campaign messages more negative and diverse? An analysis of Facebook ads in European election campaigns. https://doi.org/10.31219/osf.io/qp7dj

Papakyriakopoulos, O., Hegelich, S., Shahrezaye, M., & Serrano, J. C. M. (2018). Social media and microtargeting: Political data processing and the consequences for Germany. Big Data & Society. https://doi.org/10.1177/2053951718811844

Papakyriakopoulos, O., Shahrezaye, M., Thieltges, A., Serrano, J. C. M., & Hegelich, S. (2017). Social media und microtargeting in deutschland. Informatik-Spektrum, 40(4), 327-335. DOI: 10.1007/s00287-017-1051-4.

Prof. Dr. Pentzold, C., Fölsche, L. (2018). Die öffentliche Verhandlung von Big Data in politischen Kampagnen. ABIDA (2018). Zugriff am 18. Oktober 2021, von https://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Digitaler%20Demos.pdf

Republican National Committee. (2013). Growth and opportunity project. Letzer Zugriff 18.10.2021 http://goproject.gop.com/rncgrowthopportunitybook2013.pdf

Riahi, Y., & Riahi, S. (2018). Big data and big data analytics: Concepts, types and technologies. International Journal of Research and Engineering, 5(9), 524-528.

Sabbagh, D. (2020). Trump 2016 campaign 'targeted 3.5 m black Americans to deter them from voting'. The Guardian.

Seagate. (20. November, 2018). Prognose zum Volumen der jährlich generierten digitalen Datenmenge weltweit in den Jahren 2018 und 2025 (in Zettabyte) [Graph]. Inugriff am 18. Oktober 2021, von https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/

Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020, October). Circumvention by design-dark patterns in cookie consent for online news outlets. In Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (pp. 1-12). DOI: https://doi.org/10.1145/3419249.3420132

Strauß, S. (2020). Vom „Global Village "zur „Blackbox Society "? Digitale Identitäten und politische Kommunikation in Zeiten des Überwachungskapitalismus. Momentum Quarterly-Zeitschrift für sozialen Fortschritt, 9(2), 85-102.

Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. Internet Policy Review, 8(2).

The International Institute for Democracy and Electoral Assistance (International IDEA). #Webinar Series Report, 15 und 18 Juni 2020: Online Political Advertising and Microtargeting: The Latest Legal, Ethical, Political and Technological Evolutions https://www.idea.int/publications/catalogue/online-political-advertising-and-test-legal-ethical

Thiel, T. (2018). Digitalisierung: Gefahr für die Demokratie? Ein Essay. Politikum, 4(3), 50-55.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. First Monday, 19(7). https://doi.org/10.5210/fm.v19i7.4901

UK Information Commissioners Office (ICO). (2018, July 11). Democracy Disrupted: Personal Information and Political Influence. Online verfügbar unter https://ico.org.uk/media/action-wevetaken/2259369/democracy-disrupted-110718.pdf

Ulbricht, L. (2020). Scraping the demos. Digitalization, web scraping and the democratic project. Democratization, 27(3), 426-442. DOI: 10.1080/13510347.2020.1714595.

Zarouali, B., Dobber, T., De Pauw, G., & de Vreese, C. (2020). Using a personality-profiling algorithm to investigate political microtargeting: assessing the persuasion effects of personality-tailored ads on social media. Communication Research, 0093650220961965.

Zuiderveen Borgesius, F., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., & de Vreese, C. H. (2018). Online political microtargeting: promises and threats for democracy. Utrecht Law Review, 14(1), 82-96.

.